BASIC INDUCTION PROOFS:

In the form for our proofs by induction, in the inductive assumption we assume that \( P(n_0) \land \cdots \land P(n) \) is true then prove that \( P(n + 1) \) is true. In the most basic proofs by induction, one is often able to prove the \( n + 1 \) case by assuming only the \( k = n \) case; that is, we actually prove that \( (\forall n \geq n_0)[P(n) \rightarrow P(n + 1)] \). That will be the case in Problems 1 - 6 below.

1. Prove by induction on \( n \) that for every integer \( n \geq 1 \) we have \( \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \).

2. Prove by induction on \( n \) that for every integer \( n \geq 1 \) we have \( \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \).

3. Prove by induction on \( n \) that for every integer \( n \geq 1 \) we have \( \sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3} \).

4. Prove by induction on \( n \) that for every integer \( n \geq 1 \), 3 divides \( 2^{2n} - 1 \).

5. (a) Prove by induction on \( n \) that for every integer \( n \geq 3 \) we have \( 2n + 1 < 2^n \).

(b) Prove by induction on \( n \) that for every integer \( n \geq 5 \) we have \( n^2 < 2^n \). (Comment: At the appropriate place in proving the \( n + 1 \) case, (a) will be useful.)

6. Prove by induction on \( n \) that for every integer \( n \geq 2 \) we have \( \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n} \).

Note 1: Prove the base case without calculator assistance. Note that \( \sqrt{2} > 1 \) so \( \sqrt{2} + 1 > 2 \). Thus, division of both sides by \( \sqrt{2} \) gives \( \frac{\sqrt{2} + 1}{\sqrt{2}} > \sqrt{2} \).

Note 2: At the appropriate place in proving the \( n + 1 \) case note that \( \sqrt{n}\sqrt{n + 1} + 1 > \sqrt{n^2 + 1} = n + 1 = \sqrt{n + 1}^2 \).

Instructions for Exercises 7 and 8: Find the error in the "proofs" given in Exercises 7 and 8 below. Note that in each exercise, the statement to be proved is obviously false. It follows that the "proof" given is invalid. You are not asked to point that out. Rather, you are asked to pinpoint the error in the supposed proof and explain why it is an error.

7. Find the error in the following argument that \( 2^n = 1 \) for every integer \( n \geq 0 \).

Proof: The proof is by induction on \( n \). For \( n = 0 \) we get \( 2^0 = 2^0 = 1 \), so it is true that \( 2^n = 1 \) for \( n = 0 \).
Now let \( n \) be an integer, where \( n \geq 0 \). Assume we know that \( 2^k = 1 \) for every integer \( k \) such that \( 0 \leq k \leq n \). Then \( 2^{n+1} = 2^{n+n-(n-1)} = 2^n \cdot 2^{-(n-1)} = \frac{2^n \cdot 2^n}{2^{n-1}} \). We have assumed that \( 2^n = 1 \) and \( 2^{n-1} = 1 \). This gives \( 2^{n+1} = \frac{2^n \cdot 2^n}{2^{n-1}} = 1 \cdot 1 = 1 \). It now follows from the Principle of Induction that \( 2^n = 1 \) for every integer \( n \geq 1 \).

8. Find the error in the "proof" given below for the following statement.

For every integer \( n \geq 1 \), if \( n \) is the maximum element in the set \( \{ x, y \} \), where \( x \) and \( y \) are positive integers, then \( x = y = n \).

**Proof:** Let \( n = 1 \) and suppose that \( n \) is the maximum element in the set \( \{ x, y \} \), where \( x \) and \( y \) are positive integers. Then the only possibilities for \( x \) and \( y \) are \( x = y = 1 \).

Now let \( n \) be an integer, \( n \geq 1 \) and suppose that for every integer \( k \) with \( 1 \leq k \leq n \), if \( k \) is the maximum element in a set \( \{ x, y \} \) of positive integers, then \( x = y = k \).

Now suppose there is a set \( \{ x, y \} \) of positive integers which has \( n + 1 \) as the maximum element. Then clearly the set \( \{ x-1, y-1 \} \) has \( n \) as its maximum element. By assumption (with \( k = n \)) we have \( x-1 = y-1 = n \). Therefore, \( x = y = n + 1 \). It now follows from the Principle of Induction that for every integer \( n \geq 1 \), if \( n \) is the maximum element in the set \( \{ x, y \} \), where \( x \) and \( y \) are positive integers, then \( x = y = n \).

### Induction Proofs And Recurrence Relations

9. Define a sequence \( \{ a_n \}_{n=1}^{\infty} \) of integers by
   - \( a_1 = 1 \) and \( a_2 = 3 \).
   - For \( n \geq 3 \), \( a_n = -2a_{n-2} + 3a_{n-1} \).

Prove by induction on \( n \) that \( a_n = 2^n - 1 \) for every integer \( n \geq 1 \).

10. Let \( \{ f_i \}_{i=1}^{\infty} \) be the sequence of Fibonacci numbers. Recall that
    - \( f_1 = 1 \) and \( f_2 = 1 \).
    - For \( n \geq 3 \), \( f_n = f_{n-1} + f_{n-1} \).

   (a) Prove by induction on \( n \) that \( f_n > \frac{5}{4} f_{n-1} \) for every integer \( n \geq 3 \).
   (b) Prove by induction on \( n \) that for all integers \( n \geq 3 \) we have \( f_n > (\frac{5}{4})^n \). (Comment: At the appropriate point in proving the \( n+1 \) case, use (a).)
   (c) Prove by induction on \( n \) that \( f_n < \frac{7}{4} f_{n-1} \) for every integer \( n \geq 4 \).
   (d) Prove by induction on \( n \) that \( f_n < (\frac{7}{4})^n \) for every integer \( n \geq 4 \). (Comment: At the appropriate point in proving the \( n+1 \) case, use (c).)

Note: By (b) and (d) we have \( (\frac{5}{4})^n < f_n < (\frac{7}{4})^n \) for every integer \( n \geq 4 \).
Proofs that Require the full Inductive Assumption

11. Background:

Let $N$ denote the set of all natural numbers (i.e., the set of all positive integers). Recall that $N \times N = \{ (a, b) | a, b \in N \}$.

- For all $(a, b) \in N \times N$ set $|(a, b)| = ab$.
- We define multiplication in $N \times N$ by $(a, b)(c, d) = (ac, bd)$.

We are interested in factorization in $N \times N$. Note for example, that factorizations of $(4, 6)$ include $(4, 6) = (2, 3)(1, 2)$.

**Theorem:** For $(a, b)$ and $(c, d)$ in $N \times N$ we have $|(a, b)(c, d)| = |(a, b)|||(c, d)|$.

**Proof of Theorem:** Let $(a, b)$ and $(c, d)$ be in $N \times N$. Then $|(a, b)(c, d)| = |(ac, bd)| = |(ac)(bd)| = |(ab)(cd)| = |(a, b)|||(c, d)||$.

**Note 1:** As an immediate consequence of the definition $|(a, b)| = ab$ we see that $|(a, b)| = 1$ if and only if $(a, b) = (1, 1)$.

**Note 2:** As a consequence of the Theorem above and Note 1, we see that if $(a, b), (c, d) \in N \times N$ with $(c, d) \neq (1, 1)$ then $|(a, b)| < |(a, b)|||(c, d)| = |(ac, bd)|$.

**Definition:** An element $(a, b) \in N \times N$ is **irreducible** provided for all $(c, d)$ and $(e, f)$ in $N \times N$, if $(a, b) = (c, d)(e, f)$ then either $(c, d) = (1, 1)$ or $(e, f) = (1, 1)$.

**Examples:** $(2, 1), (1, 2), (1, 5), (5, 1)$ are examples of irreducible elements in $N \times N$. On the other hand, $(2, 3)$ is reducible since $(2, 3) = (2, 1)(1, 3)$.

**Exercise 11a:** Complete the following definition, given that reducible means not irreducible:

An element $(a, b) \in N \times N$ is **reducible** provided . . .

**Exercise 11b:** Prove by induction on $n = |(a, b)|$ that for all $(a, b) \in N \times N$, if $|(a, b)| = n \geq 2$ then either $(a, b)$ is irreducible or $(a, b)$ can be expressed as the product of two or more irreducible elements in $N \times N$.

The Division Algorithm and GCD’s

12. In each (a) – (d) you are given integers $m$ and $d$ where $d$ is positive. In each case find integers $q$ and $r$ such that $m = qd + r$ and $0 \leq r \leq d$.

(a) $m = 31$ and $d = 62$  
(b) $m = -83$ and $d = 255$

(c) $m = 751$ and $d = 92$  
(d) $m = -1097$ and $d = 112$. 

3
13. In each of (a) – (d) find \( d = \gcd(a, b) \) then express \( d \) in the form \( d = ma + nb \), where \( m \) and \( n \) are integers.

(a) \( a = 9299 \) and \( b = 547 \) 
(b) \( a = 78043 \) and \( b = 3381 \) 
(c) \( a = 37098 \) and \( b = 11610 \) 
(d) \( a = -37098 \) and \( b = 11610 \)

14. In each of the following determine \( d = \gcd(a, b) \). Justify your answer.

(a) There exist integers \( m, n, r, \) and \( s \) such that \( 5 = ma + nb \) and \( 7 = ra + sb \).
(b) 5 divides both \( a \) and \( b \) and there exist integers \( m, n, r, \) and \( s \) such that \( 15 = ma + nb \) and \( 20 = ra + sb \).
(c) 3 is not a common divisor of \( a \) and \( b \), \( 1 \neq \gcd(a, b) \) and there exist integers \( m, n, r, \) and \( s \) such that \( 30 = ma + nb \) and \( 105 = ra + sb \).

15. Let \( a \) and \( b \) be integers and suppose that \( d = \gcd(a, b) \). Let \( m \) and \( n \) be integers such that \( m = qa + rb \) and \( n = sa + tb \) for some integers \( q, r, s, \) and \( t \). Suppose further that there are integers \( u \) and \( v \) such that \( d = um + vn \). Prove that \( d = \gcd(m, n) \).

16. Let \( a, b, \) and \( c \) be integers.

**Definition:** A positive integer \( d \) is the greatest common divisor of \( a, b, \) and \( c \) provided:

1. \( d \) divides each of \( a, b, \) and \( c \), and;
2. If \( m \) is an integer that divides each of \( a, b \) and \( c \), then \( m \) divides \( d \).

**Exercise 16:** Let \( a, b, \) and \( c \) be nonzero integers. Let \( d = \gcd(a, b) \) and let \( q = \gcd(d, c) \).
[So \( q = \gcd(\gcd(a, b), c) \).] Prove that \( q = \gcd(a, b, c) \)

17. If \( a, b, \) and \( c \) are integers and \( q = \gcd(a, b, c) \), prove that there exist integers \( l, m, \) and \( n \) such that \( q = la + mb + nc \). (Hint: Use Exercise 14 above and Theorem 4 of Section 4.2).

18. Find \( d = \gcd(1995, 450, 153) \) and express \( d \) in the form \( d = l \cdot 1995 + m \cdot 450 + n \cdot 153 \).

19. Let \( a \) and \( b \) be relatively prime integers; that is, assume that \( 1 = \gcd(a, b) \).

(a) Prove by induction on \( n \) that \( 1 = \gcd(a, b^n) \) for every integer \( n \geq 1 \). [When proving the \( n + 1 \) case, recall from the 4.3 Exercises that if \( 1 = \gcd(a, b) \) and \( 1 = \gcd(a, c) \) then \( 1 = \gcd(a, bc) \).]

(b) Let \( m \) be a positive integer. Prove that \( 1 = \gcd(a^n, b^m) \) for every integer \( n \geq 1 \). [Note: This is not a proof by induction. First use (a) to observe that \( 1 = \gcd(a, b^n) \) then use (a) to conclude that \( 1 = \gcd(a^n, b^m) \) for every integer \( n \geq 1 \).]

**Note:** We conclude from (b) above that if \( 1 = \gcd(a, b) \), then \( 1 = \gcd(a^n, b^m) \) for every integer \( n \geq 1 \).

20. Let \( a \) and \( b \) be nonzero integers and suppose that \( d = \gcd(a, b) \). Prove that for every integer \( n \geq 1 \) we have \( d^n = \gcd(a^n, b^n) \). [Hint: Use Exercise 4.3.1 and the note following Exercise 19b above.]
SOLUTIONS

Proof of 1:

The proof is by induction on \( n \). For \( n = 1 \) we have \( \sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 \) and

\[
\frac{n(n+1)}{2} = \frac{1 \cdot 2}{2} = 1.
\]

Therefore, the desired equality holds when \( n = 1 \).

An Aside: I will state the full inductive assumption but, as noted above, we will only require the assumption when \( k = n \).

Let \( n \) be an arbitrary integer \( n \geq 1 \). Assume we know that \( \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \) for every integer \( k \) such that \( 1 \leq k \leq n \). In particular, for \( k = n \) we are assuming that \( \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \).

Note that

\[
\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n + 1) = \frac{n(n+1)}{2} + (n + 1) = \frac{n(n+1) + 2(n + 1)}{2} = \frac{(n+1)(n+2)}{2}.
\]

This proves that the desired equality holds for \( n + 1 \) so, by the Principle of Mathematical Induction, for every integer \( n \geq 1 \) we have \( \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \).

Proof of 2:

The proof is by induction on \( n \). For \( n = 1 \) we have \( \sum_{i=1}^{n} i^2 = \sum_{i=1}^{1} i^2 = 1^2 = 1 \) and

\[
\frac{n(n+1)(2n+1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1.
\]

Therefore, the desired equality holds when \( n = 1 \).

Let \( n \) be an arbitrary integer \( n \geq 1 \). Assume we know that \( \sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6} \) for every integer \( k \) such that \( 1 \leq k \leq n \). In particular, for \( k = n \) we are assuming that \( \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \).

Note that

\[
\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n + 1)^2 = \frac{n(n+1)(2n+1)}{6} + (n + 1)^2
\]

\[
= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} = \frac{(n+1)(2n^2 + 7n + 6)}{6}
\]

\[
= \frac{(n+1)(n+2)(2n+3)}{6} = \frac{(n+1)[(n+1) + 1][2(n+1) + 1]}{6}.
\]

This proves that the desired equality holds for \( n + 1 \) so, by the Principle of Mathematical Induction, for every integer \( n \geq 1 \) we have \( \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \).
Proof of 3:

The proof is by induction on \( n \). For \( n = 1 \) we have \( \sum_{i=1}^{n} i(i + 1) = \frac{1}{3} i(i + 1) = 1 \cdot 2 = 2 \) and \( n(n + 1)(n + 2) \). Therefore, the desired equality holds when \( n = 1 \).

Let \( n \) be an arbitrary integer \( n \geq 1 \). Assume we know that \( \sum_{i=1}^{k} i(i + 1) = \frac{k(k + 1)(k + 2)}{3} \) for every integer \( k \) such that \( 1 \leq k \leq n \). In particular, for \( k = n \) we are assuming that \( \sum_{i=1}^{n} i(i + 1) = \frac{n(n + 1)(n + 2)}{3} \).

Note that \( \sum_{i=1}^{n+1} i(i + 1) = \sum_{i=1}^{n} i(i + 1) + (n + 1)(n + 2) = \frac{n(n + 1)(n + 2)}{3} + (n + 1)(n + 2) = \frac{n(n + 1)(n + 2) + 3(n + 1)(n + 2)}{3} = \frac{(n + 1)(n + 1 + 1)(n + 1 + 2)}{3} \). This proves that the desired equality holds for \( n + 1 \) so, by the Principle of Mathematical Induction, for every integer \( n \geq 1 \) we have \( \sum_{i=1}^{n} i(i + 1) = \frac{n(n + 1)(n + 2)}{3} \).

Proof of 4:

The proof is by induction on \( n \). For \( n = 1 \) we get \( 2^{2n} - 1 = 2^2 - 1 = 4 - 1 = 3 \) so for \( n = 1 \) the quantity \( 2^{2n} - 1 \) is clearly divisible by 3.

Let \( n \) be an arbitrary integer, \( n \geq 1 \). Suppose we know that \( 2^{2k} - 1 \) is divisible by 3 for every integer \( k \) such that \( 1 \leq k \leq n \). In particular (with \( k = n \)) assume we know that \( 2^{2n} - 1 = 3m_n \) for some integer \( m_n \).

Then \( 2^{2(n+1)} - 1 = 2^{2n+2} - 1 = 2^{2n}2^2 - 1 = 2^{2n}4 - 1 = 2^{2n}4 - 4 + 4 - 1 = 4(2^{2n} - 1) + 3 = 4 \cdot 3m_n + 3 = 3(4m_n + 1) \). Consequently, 3 divides \( 2^{2(n+1)} - 1 \).

By the Principle of Mathematical Induction, 3 divides \( 2^{2n} - 1 \) for every integer \( n \geq 1 \).

Proof of 5:

(a) The proof is by induction on \( n \). For \( n = 3 \) we note that \( 2n + 1 = 2(3) + 1 = 7 \) whereas \( 2^n = 2^3 = 8 \). Clearly \( 7 < 8 \) so for \( n = 3 \) we get \( 2n + 1 < 2^n \).

Now let \( n \) be an integer such that \( n \geq 3 \). Assume we know that \( 2k + 1 < 2^k \) for every integer \( k \) such that \( 3 \leq k \leq n \). In particular, for \( k = n \), we are assuming that \( 2n + 1 < 2^n \).

Now \( 2(n + 1) + 1 = 2n + 3 = (2n + 1) + 2 < 2^n + 2 < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1} \). Therefore, \( 2(n + 1) + 1 < 2^{n+1} \) so, by the Principle of Induction, \( 2n + 1 < 2^n \) for every integer \( n \geq 3 \).

(b) The proof is by induction on \( n \). For \( n = 5 \) we have \( n^2 = 5^2 = 25 \) and \( 2^n = 2^5 = 32 \). Clearly \( 25 < 2^5 \) so for \( n = 1 \) we get \( n^2 < 2^n \).

Now let \( n \) be an integer such that \( n \geq 5 \). Assume we have already shown that \( k^2 < 2^k \) for every integer \( k \) such that \( 5 \leq k \leq n \). In particular, with \( k = n \), assume we know that \( n^2 < 2^n \).
Now \((n + 1)^2 = n^2 + 2n + 1 < 2^n + 2n + 1\). By (a), \(2n + 1 < 2^n\) for \(n \geq 3\). Since we are assuming that \(n \geq 5\) we now have \((n + 1)^2 < 2^n + 2n + 1 < 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}\). This proves that \((n + 1)^2 < 2^{n+1}\). By the Principle of Mathematical Induction, we now know that \(n^2 < 2^n\) for every integer \(n \geq 5\).

**Proof of 6:**

The proof is by induction on \(n\). For \(n = 2\) the sum \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}}\) becomes \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}}\). We need to prove that \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} > \sqrt{2}\). We know that \(\sqrt{2} > 1\) so \(\sqrt{2} + 1 > 2\). Division of both sides by \(\sqrt{2}\) gives \(\frac{\sqrt{2} + 1}{\sqrt{2}} > \sqrt{2}\). Thus \(\frac{\sqrt{2} + 1}{\sqrt{2}} > \sqrt{2}\). But \(\frac{\sqrt{2}}{\sqrt{2}} = 1 = \frac{1}{\sqrt{1}}\). Therefore, \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} > \sqrt{2}\) and the base case is proved.

Now let \(n\) be an integer, \(n \geq 2\). Assume we know that \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{k}} > \sqrt{k}\) for every integer \(k\) such that \(2 \leq k \leq n\). In particular (with \(k = n\)) we are supposing we know that \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}\).

Now
\[
\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} = \left(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}}\right) + \frac{1}{\sqrt{n+1}} > \sqrt{n} + \frac{1}{\sqrt{n+1}}
\]
\[
= \frac{\sqrt{n}\sqrt{n+1} + 1}{\sqrt{n+1}} > \frac{\sqrt{n}\sqrt{n+1}}{\sqrt{n+1}} = \frac{n + 1}{\sqrt{n+1}} = \frac{\sqrt{n+1}^2}{\sqrt{n+1}} = \sqrt{n+1}.
\]

By the Principle of Mathematical Induction, it follows that \(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}\) for every integer \(n \geq 2\).

**Solution to 7:**

The error in the proof occurs in the proof of the \(n + 1\) case where it is stated that "we have assumed that \(2^n = 1\) and \(2^{n-1} = 1\)." The assumption that \(2^n = 1\) is okay, but the assumption that \(2^{n-1} = 1\) is not. In the inductive assumption we have assumed that \(n \geq 0\), so our proof of the \(n + 1\) case must be valid for the case \(n = 0\); that is, for the case when \(n + 1 = 1\). In this case, \(n - 1 = -1\) and we have neither proved nor assumed that \(2^{-1} = 1\).

**Solution to 8:**

In the \(n + 1\) case we assume that \(n + 1\) is the maximum element in the set \(\{x, y\}\), where \(x\) and \(y\) are positive integers. We then conclude, correctly, that \(n\) is the maximum element in the set \(\{x - 1, y - 1\}\). However, \(x - 1\) and \(y - 1\) may no longer both be positive integers, in which case the inductive assumption does not apply.

To illustrate, suppose \(n = 1\), so \(n + 1 = 2\). Now 2 is the maximum element of the set \(\{1, 2\}\) and 1 is the maximum element in the set \(\{1 - 1, 2 - 1\} = \{0, 1\}\). The resulting integers are not both positive, however, so the \(n = 1\) case does not apply.
Proof of 9:

The proof is by induction on $n$, where $n \geq 1$.

For $n = 1$ we have $a_n = a_1 = 1$ and $2^n - 1 = 2 - 1 = 1$. Therefore $a_n = 2^n - 1$ for $n = 1$.

For $n = 2$ we have $a_n = a_2 = 3$ and $2^n - 1 = 2^2 - 1 = 4 - 1 = 3$. Therefore $a_n = 2^n - 1$ for $n = 2$.

Now let $n$ be an integer, $n \geq 2$ and assume we know that $a_k = 2^k - 1$ for every integer $k$ such that $1 \leq k \leq n$.

Since $n \geq 2$, we have $n + 1 \geq 3$ so $a_{n+1}$ is defined by the recurrence relation; that is, $a_{n+1} = -2a_{n-1} + 3a_n$. Again, since $n \geq 2$, we have $n - 1 \geq 1$ so $1 \leq n - 1 < n \leq n$ and we have assume that $a_k = 2^k - 1$ for every integer $k$ such that $1 \leq k \leq n$. In particular, then, we have assumed that $a_{n-1} = 2^{n-1} - 1$ and $a_n = 2^n - 1$. This gives

$$a_{n+1} = -2a_{n-1} + 3a_n = -2(2^{n-1} - 1) + 3(2^n - 1) = (-2^n + 2) + (3 \cdot 2^n - 3) = 2 \cdot 2^n - 1 = 2^{n+1} - 1.$$  

By the Principle of Mathematical Induction, $a_n = 2^n - 1$ for every integer $n \geq 1$.

Solution to 10:

Solution to (a): First we do some construction. When we prove the $n + 1$ case it will be convenient to use the recurrence relation $f_{n+1} = f_n + f_{n-1}$. This will require that $n + 1 \geq 3$ which will automatically be true since we begin with $n \geq 3$. Next, we want our inductive assumption to include $f_n$ and $f_{n-1}$. This requires that $n - 1 \geq 3$ or $n \geq 4$.

Therefore, our base cases are $n = 3$ and $n = 4$.

Proof of (a): The proof is by induction on $n$. For $n = 3$ we have $f_n = f_3 = 2$ and

$$\frac{5}{4}f_{n-1} - \frac{5}{4}f_2 = \frac{5}{4} \cdot 1 = \frac{5}{4}.\text{Clearly } 2 > \frac{5}{4}\text{ so for }n = 3\text{ we have proved that }f_n > \frac{5}{4}f_{n-1}.\text{ For }n = 4\text{ we have }f_n = f_4 = 3\text{ and }\frac{5}{4}f_{n-1} - \frac{5}{4}f_3 = \frac{5}{4} \cdot 2 = \frac{5}{2}.\text{ Clearly }3 > \frac{5}{2}\text{ so for }n = 4\text{ we have proved that }f_n > \frac{5}{4}f_{n-1}.$$

Now let $n$ be an integer such that $n \geq 4$ and suppose we know that $f_k > \frac{5}{4}f_{k-1}$ for every integer $k$ such that $3 \leq k \leq n$.

Since $n \geq 4$, $n + 1 \geq 5$ and $f_{n+1}$ is defined by the recurrence relation; that is, $f_{n+1} = f_n + f_{n-1}$. Our inductive assumption applies to both $k = n$ and $k = n - 1$ since $n - 1 \geq 4 - 1 = 3$. Thus, we have assumed that $f_n > \frac{5}{4}f_{n-1}$ and $f_{n-1} > \frac{5}{4}f_{n-2}$. This gives us

$$f_{n+1} = f_n + f_{n-1} = \frac{5}{4}f_{n-1} + \frac{5}{4}f_{n-2} = \frac{5}{4}(f_{n-1} + f_{n-2}) = \frac{5}{4}f_n.\text{ It now follows from the Principle of Mathematical Induction that }f_n > \frac{5}{4}f_{n-1}\text{ for every integer }n \geq 3.$$

Proof of (b): (An Aside: In proving the $n + 1$ case we will use (a) and not the recurrence relation, so our base case will be $n = 3$.)

The proof is by induction on $n$. For $n = 3$ we have $f_n = f_3 = 2$ and $(\frac{5}{4})^n = (\frac{5}{4})^3 = \frac{125}{64}$. Now

$$2 = \frac{125}{64} > \frac{125}{64} = (\frac{5}{4})^3, \text{ so for }n = 3\text{ we have }f_n > (\frac{5}{4})^n.$$

Now let $n$ be an integer with $n \geq 3$ and assume we know that $f_k > (\frac{5}{4})^k$ for every integer $k$ such that $3 \leq k \leq n$. In particular (with $k = n$) we are assuming that $f_n > (\frac{5}{4})^n$.

Since $n \geq 3$ by assumption, $n + 1 \geq 4$. In particular, (a) above applies and

$$f_{n+1} > \frac{5}{4}f_n > \frac{5}{4}(\frac{5}{4})^n = (\frac{5}{4})^{n+1}.\text{ By the Principle of Induction we conclude that }f_n > (\frac{5}{4})^n\text{ for every integer }n \geq 3.$$
Proof of (c): An aside: This proof is similar to (a) except it begins at \( n = 4 \). As in (a) we need two base cases, \( n = 4 \) and \( n = 5 \).

The proof is by induction on \( n \). For \( n = 4 \) we have \( f_n = f_4 = 3 \) and \( \frac{7}{4} f_n - 1 = \frac{7}{4} f_3 = \frac{7}{4} \cdot 2 = \frac{7}{2} \). Clearly \( 3 < \frac{7}{2} \) so for \( n = 4 \) we have proved that \( f_n < \frac{7}{4} f_n - 1 \). For \( n = 5 \) we have \( f_n = f_5 = 5 \) and \( \frac{7}{4} f_n - 1 = \frac{7}{4} f_4 = \frac{7}{4} \cdot 3 = \frac{21}{4} \). Clearly \( 5 < \frac{21}{4} \) so for \( n = 5 \) we have proved that \( f_n < \frac{7}{4} f_n - 1 \).

Now let \( n \) be an integer such that \( n \geq 5 \) and suppose we know that \( f_k < \frac{7}{4} f_{k-1} \) for every integer \( k \) such that \( 4 \leq k \leq n \).

Since \( n \geq 5 \), \( n + 1 \geq 6 \) and \( f_{n+1} \) is defined by the recurrence relation; that is,

\[ f_{n+1} = f_n + f_{n-1}. \]

Our inductive assumption applies to both \( k = n \) and \( k = n - 1 \) since \( n - 1 \geq 5 - 1 = 4 \). Thus, we have assumed that \( f_n < \frac{7}{4} f_{n-1} \) and \( f_{n-1} < \frac{7}{4} f_{n-2} \). This gives us

\[ f_{n+1} = f_n + f_{n-1} < \frac{7}{4} f_{n-1} + \frac{7}{4} f_{n-2} = \frac{7}{4} (f_{n-1} + f_{n-2}) = \frac{7}{4} f_n. \]

It now follows from the Principle of Mathematical Induction that \( f_n < \frac{7}{4} f_{n-1} \) for every integer \( n \geq 4 \).

Proof of (d): The proof is by induction on \( n \). For \( n = 4 \) we have \( f_n = f_4 = 3 \) and

\[ \left( \frac{7}{4} \right)^4 = \left( \frac{7}{4} \right)^4 = \frac{7^4}{4^4} = \frac{2401}{256}. \]

Now \( 3 = \frac{818}{256} < \frac{2401}{256} = \left( \frac{7}{4} \right)^4 \), so for \( n = 4 \) we have \( f_n < \left( \frac{7}{4} \right)^n \).

Now let \( n \) be an integer with \( n \geq 4 \) and assume we know that \( f_k < \left( \frac{7}{4} \right)^k \) for every integer \( k \) such that \( 4 \leq k \leq n \). In particular (with \( k = n \)) we are assuming that \( f_n < \left( \frac{7}{4} \right)^n \).

Since \( n \geq 4 \) by assumption, \( n + 1 \geq 4 \). In particular, (c) above applies and \( f_{n+1} < \frac{7}{4} f_n < \left( \frac{7}{4} \right)^n \left( \frac{7}{4} \right)^{n+1} = \left( \frac{7}{4} \right)^{n+1} \). By the Principle of Induction we conclude that \( f_n < \left( \frac{7}{4} \right)^n \) for every integer \( n \geq 4 \).

Solution to 11a:

An element \((a, b) \in N \times N\) is reducible provided there exists elements \((c, d)\) and \((e, f)\) in \(N \times N\) such that \((a, b) = (c, d)(e, f)\) and \((c, d) \neq (1, 1)\) and \((e, f) \neq (1, 1)\).

Proof of 11b:

The proof is by induction on \( n = \|(a, b)\| \) where \( n \geq 2 \). Suppose \((a, b) \in N \times N\) with \( \|(a, b)\| = 2 \). Then either \((a, b) = (1, 2)\) or \((a, b) = (2, 1)\). In either case, \((a, b)\) is irreducible and we are done.

Now let \( n \geq 2 \) and assume we know that if \((a, b) \in N \times N\) and \( \|(a, b)\| = k \), where \( 2 \leq k \leq n \), then either \((a, b)\) is irreducible or \((a, b)\) can be expressed as a product of two or more irreducible elements in \(N \times N\).

Now suppose \((a, b) \in N \times N\) and \( \|(a, b)\| = n + 1 \). If \((a, b)\) is irreducible then we are done. Thus, assume that \((a, b)\) is reducible. Then there exists elements \((c, d)\) and \((e, f)\) in \(N \times N\) such that \((a, b) = (c, d)(e, f)\) and \((c, d) \neq (1, 1)\) and \((e, f) \neq (1, 1)\). It follows that \( 2 \leq \|(c, d)\| \leq \|(a, b)\| = n + 1 \). Hence, if \( l = \|(c, d)\| \) then \( 2 \leq l \leq n \). Similarly \( 2 \leq \|(e, f)\| \leq \|(a, b)\| = n + 1 \). Hence, if \( m = \|(e, f)\| \) then \( 2 \leq m \leq n \). By the inductive assumption, each of \((c, d)\) and \((e, f)\) is either irreducible or can be expressed as a product of two or more irreducible elements from \(N \times N\). Consequently, \((a, b) = (c, d)(e, f)\) can be expressed as a product of two or more irreducible elements from \(N \times N\). By the Principle of Mathematical Induction, for all \((a, b) \in N \times N\) if \( \|(a, b)\| \geq 2 \) then either \((a, b)\) is irreducible or \((a, b)\) can be expressed as a product of two or more irreducible elements from \(N \times N\).
Solution to 12:
(a) \( 31 = (0)62 + 31 \) so \( q = 0 \) and \( r = 31 \).
(b) \(-83 = (0)255 - 83 = -255 + 255 - 83 = (-1)255 + 172 \), so \( q = -1 \) and \( r = 172 \).
(c) \( 751 = (8)92 + 15 \) so \( q = 8 \) and \( r = 15 \).
(d) \( 1097 = (9)112 + 89 \) so 
\(-1097 = (-9)112 - 89 = (-9)112 - 112 + 112 - 89 = (-10)112 + 23 \). Therefore, \( q = -10 \) and \( r = 23 \).

Solution to 13:
(a) \( 9299 = (17)547 \) so \( 547 = \gcd(9299, 547) \). We have \( 547 = (0)9299 + (1)547 \).

(b) The divisions are: \( 78043 = (23)3381 + 280 \), \( 3381 = (12)280 + 21 \), \( 280 = (13)21 + 7 \) and \( 7 \) divides \( 21 \) so \( 7 = \gcd(78043, 3381) \).

Rewriting the equations obtained from the divisions gives: \( 7 = 280 + (-13)21 \), \( 21 = 3381 + (-12)280 \), \( 280 = 78043 + (-13)3381 \). So 
\( 7 = (157)78043 + (-3624)3381 \).

(c) The divisions are: \( 37098 = (3)11610 + 2268 \), \( 11610 = (5)2268 + 270 \), \( 2268 = (8)270 + 108 \), \( 270 = (2)108 + 54 \), and \( 108 = (2)54 \), so \( 54 = \gcd(37098, 11610) \).

Rewriting the equations obtained from the divisions gives: \( 54 = 270 + (-2)108 \), \( 108 = 2268 + (-8)270 \), \( 270 = 11610 + (-5)2268 \), and \( 2268 = 37098 + (-3)11610 \).

Using the equations in the order given above, we get: 
\( 54 = 270 + (-2)108 = 270 + (-2)[2268 + (-8)270] = (-2)2268 + (17)270 = 
(-2)2268 + (17)[11610 + (-5)2268] = (17)11610 + (-87)2268 = 
(17)11610 + (-87)[37098 + (-3)11610] = (-87)37098 + (278)11610 \). Thus, 
\( 54 = (-87)37098 + (278)11610 \).

(d) It follows from (c) that \( 54 = \gcd(-37098, 11610) \) and from (c) we get 
\( 54 = (-87)37098 + (278)11610 = (87)(-37098) + (278)11610 \).

Solution to 14:
(a) Let \( d = \gcd(a, b) \). Since \( 5 = ma + nb \) and \( 7 = ra + sb \), both 5 and 7 are multiples of \( d \).
But \( 1 = \gcd(5, 7) \), so \( d \) divides 1. Consequently, \( d = 1 \).

(b) Let \( d = \gcd(a, b) \). Since 5 is given to be a common divisor of \( a \) and \( b \), we know that \( d \) must be a multiple of 5 – say \( d = 5q \). Since \( 15 = ma + nb \) and \( 20 = ra + sb \), both 15 and 20 are multiples of \( d \). Thus, there exist integers \( k \) and \( l \) such that \( 15 = kd = k(5q) \) and \( 20 = ld = l(5q) \). This gives \( 3 = kq \) and \( 4 = lq \); that is, \( q \) is a common divisor of 3 and 4.
But 3 and 4 are clearly relatively prime, so \( q = 1 \). Therefore, \( d = 5q = 5 \).

(c) Let \( d = \gcd(a, b) \). Since 3 is not a common divisor of \( a \) and \( b \), 3 is not a divisor of \( d \).
(If 3 divides \( d \) then \( d \) divides both \( a \) and \( b \), so 3 divides both \( a \) and \( b \).) Since 3 is prime, \( d \)
and 3 are relatively prime. Since 30 = ma + nb and 105 = ra + sb, both 30 and 105 are multiples of d. Thus, d divides 30 = 3 \cdot 10 and d divides 105 = 3 \cdot 35. Since d and 3 are relatively prime, d divides 10 and d divides 35. Now 5 = gcd(10, 35) and d is a common divisor of 10 and 35 so d divides 5. Thus, either d = 1 or d = 5. But 1 ≠ gcd(a, b), so d = 5.

Proof of 15:
Since d = um + vn we know that d is a multiple of gcd(m, n). Likewise, since d = gcd(a, b) and m = qa + rb, m is a multiple of d. Also, n = sa + tb so n is a multiple of d. Thus, d is a common divisor of m and n, so d divides gcd(m, n). It follows that d = gcd(m, n).

Proof of 16:
Let a, b, and c be integers, let d = gcd(a, b) and let q = gcd(d, c). We must prove that q = gcd(a, b, c).

We first show that q is a common divisor of a, b, and c. But q = gcd(d, c) so q divides both d and c. But d = gcd(a, b) so d divides both a and b. Since q divides d and d divides both a and b, it follows that q divides both a and b. This proves that q is a common divisor of a, b, and c.

Now let k be a common divisor of a, b, and c. We must show that k divides q. Since k is a common divisor of a and b and d = gcd(a, b), it follows that k divides d. Thus, k is a common divisor of d and c. But q = gcd(d, c) so it follows that k divides q.

It now follows from the definition given above that q = gcd(a, b, c).

Proof of 17:
Let a, b, and c be integers and suppose that q = gcd(a, b, c). Set d = gcd(a, b). We know from Exercise 16 that q = gcd(d, c). By Theorem 4 of Section 4.2 there exist integers r and n such that q = rd + nc. Likewise, since d = gcd(a, b), there are integers x and y such that d = xa + yb. It now follows that q = rd + nc = (rx)a + (ry)b + nc. With l = rx and m = ry we have q = la + mb + nc.

Solution to 18:
Following the result of Exercise 16, we first calculate gcd(1995, 450). The divisions are:

Let’s now rewrite the division equations as:
15 = 195 + (−3)60, 60 = 450 + (−2)195, and 195 = 1995 + (−4)450. From these equations, taken in order, we get:
15 = 195 + (−3)60 = 195 + (−3)[450 + (−2)195] = (−3)450 + (7)195 = (−3)450 + (7)[1995 + (−4)450] = (7)1995 + (−31)450.

In summary,
15 = (7)1995 + (−31)450.

We now know, from Exercise 16, that gcd(1995, 450, 153) = gcd(153, 15). The only division for this problem is: 153 = (10)15 + 3. Since 3 divides 15, 3 = gcd(153, 15). Moreover, 3 = (1)153 + (−10)15.
We now know that $3 = \gcd(1995, 450, 153)$. We have
$$3 = (1)153 + (-10)15 = (1)153 + (-10)[(7)1995 + (-31)450].$$ So
$$3 = (-70)1995 + (310)450 + (1)153.$$ 

**Solution to 19:**

**Proof of a:** The proof is by induction on $n$. The case $n = 1$ is given; that is, $1 = \gcd(a, b)$ is given. Now assume that $n$ is an integer with $n \geq 1$ and suppose we know that $1 = \gcd(a, b^k)$ for every integer $k$ such that $1 \leq k \leq n$. In particular, we now have $1 = \gcd(a, b)$ and $1 = \gcd(a, b^n)$. By an exercise from Section 4.2, it follows that $1 = \gcd(a, b \cdot b^n) = \gcd(a, b^{n+1})$. By the Principle of Mathematical Induction, $1 = \gcd(a, b^n)$ for every integer $n \geq 1$.

**Proof of b:** It follows from (a) that $1 = \gcd(a, b^m)$. It now follows from (a) [let $b^m$ play the role played by $a$ in (a) and let $a$ play the role played by $b$ in (a)] that for every integer $n \geq 1$ we have $1 = \gcd(a^n, b^n)$.

**Proof of 20:**

Suppose $d = \gcd(a, b)$ and $a = a_1d$ and $b = b_1d$. If $n$ is an integer with $n \geq 1$ then $a^n = a_1^n d^n$ and $b^n = b_1^n d^n$. By Exercise 4.3.1, $1 = \gcd(a_1, b_1)$. Thus, by Exercise 19 above, $1 = \gcd(a_1^n, b_1^n)$. Again by Exercise 4.3.1 (applied to $d^n$, $a^n$, $b^n$, $a_1^n$ and $b_1^n$) we conclude that $d^n = \gcd(a^n, b^n)$.

Alternatively, it is clear that $d^n$ is a common divisor of $a^n$ and $b^n$ as shown above. But there exist integers $r$ and $s$ such that $1 = ra_1^n + sb_1^n$. Therefore, $d^n = d^n \cdot 1 = d^n(ra_1^n + sb_1^n) = r(d^n a_1^n) + s(d^n b_1^n) = ra^n + sb^n$. It follows that $d^n = \gcd(a^n, b^n)$. 

12